IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Luz Maria Camacho et al.	Confirmation No. 4973
Serial No.: 09/801,468	Examiner: Brown, Christopher J. Art Unit: 2134
Filed: March 7, 2001	Atty. Docket No. 010942-0269936 AWT-003

For: Method and Apparatus for Reducing On-Line Fraud Using Personal Digital Identification

Submitted electronically on May 30, 2006

BRIEF ON APPEAL

Mail Stop APPEAL
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This paper is further to the Notice of Appeal dated March 28, 2006, for which a supportive brief is due May 30, 2006 (May 28 = Sunday, May 29 = Holiday). Applicant claims small entity status, see 37 CFR 1.27. The Commissioner is authorized to charge the small entity fee for filing a brief in support of an appeal in the amount of $250.00, and any required fee to Pillsbury Winthrop Shaw Pittman LLP's deposit account no. 03-3975 (order no. 010942-0269936).

REAL PARTY IN INTEREST

The real party in interest is Aurora Wireless Technologies, Ltd., which has full title to the present application by virtue of an assignment from the inventors recorded at Reel/Frame No. 011589/0350.

RELATED APPEALS AND INTERFERENCES

There are no appeals or interferences that will directly affect, be directly affected by, or have a bearing on the Board's decision in this appeal.

STATUS OF CLAIMS

Claims 1, 2, 4-8, 10-16, 18-21, 23-27, 29-35, 37-40, 43 and 45-51 are pending in the application. Claims 1, 2, 4-8, 10-16, 18-21, 23-27, 29-35, 37-40, 43 and 45-51 stand rejected two or more times; claims 3, 9, 17, 22, 28, 36, 41-42 and 44 are canceled. The repeated and unfounded rejections of all pending claims 1, 2, 4-8, 10-16, 18-21, 23-27, 29-35, 37-40, 43 and 45-51 are appealed.

STATUS OF AMENDMENTS

An amendment to cure a newly-discovered informality in claim 50 is being submitted concurrently with this Appeal. No amendments were filed in response to the last Office Action mailed January 13, 2006.

SUMMARY OF CLAIMED SUBJECT MATTER

The present invention relates to reducing on-line fraud, and more particularly to a method and apparatus for authenticating on-line transactions using stored authentication rules for a plurality of businesses. (see the present specification at, for example, page 4, line 15 to page 5, line 10)

One aspect of the invention relates to providing a centralized, service bureau authentication facility for a plurality of companies. (see, for example, page 9, lines 8-18) An example implementation of this embodiment is PDI system 100 as further illustrated in FIG. 2.

In general operation of the example embodiment in FIG. 2, a PDI web-enabled server 204 accepts the purchase request from authorized electronic storefront sites. The request is first processed to ensure that business-filtering rules are applied to the transaction by way of the Filter Manager 208. This filtering process quickly identifies those transactions that warrant further authentication, or which may be immediately rejected by the system. Thereafter, a Transaction Rules Manager 212 processes the request. For example, the Transaction Rules Manager 212 processes the request against company level (i.e. business) rules to determine if authentication is required and, if so, what type should be requested of the consumer. After this determination, the resultant data is forwarded to the Authentication Manager 216 which, if required, initiates a dialog with the client 102, and collects and evaluates the authentication data (typically a biometric indicia such as a fingerprint) against stored templates. If the authentication data is properly collected and authenticated, the request is forwarded to the credit payment service 206 for approval of credits and debits. If the request is not properly authenticated, the requestor and the electronic storefront 202 are notified, and the purchase transaction does not complete. The consumer must re-submit the transaction request again, if permitted to do so. (see the present specification at, for example, page 12, line 15 to page 13, line 14).

The invention thus provides an effective and efficient system that can quickly isolate those individual transactions that are associated with on-line fraud, while providing a mechanism that can accurately authenticate individuals who are authorized to performs such transactions.

In accordance with certain aspects of the invention, and as set forth in independent claims 1, 20 and 39, a method and system includes storing business rules (e.g. configuration files 402) for a plurality of companies (e.g. electronic storefront 202) having on-line resources (e.g. Internet 104 accessed services such as on-line voting, e-commerce, on-line banking, on-line trading, auctions, premium services and access control); receiving a message indicating a request from a user (e.g. consumer interacting with electronic storefront 202 with client 102) to use on-line resources; identifying a company (e.g. electronic storefront 202) associated with the requested on-line resource from among the plurality of companies (e.g. merchant domain identity, block S402); retrieving the stored business rules (e.g. configuration files 402) for the identified company (e.g. "mapping" form file, block S408); determining whether the request requires authentication (e.g. block S308); enabling the request to be fulfilled without authentication if the

determination indicates that authentication is not required (e.g. block S316); obtaining an indicia of physical identification from the user if the determination instead indicates that authentication is required (e.g. blocks S310 and S312); comparing the obtained indicia to a stored indicia (e.g. biometric template from biometric database, blocks S922 and S924) for the user; and enabling the request to be fulfilled if the obtained indicia matches the stored indicia (blocks S314 and S316), wherein the step of determining whether the request requires authentication includes determining whether stored business rules for the identified company associated with the requested on-line resource indicates that authentication for the user is required (e.g. operations of Transaction Rules Manager 214, see FIGs.7A, B and C, page 29, line 9 to page 33, line 7).

In addition, as further set forth in dependent claims 2, 21 and 40, a process for determining whether authentication is required includes storing a profile of a user's authentication patterns (e.g. historical usage counts stored in subsystem 220, see page 36, lines 12-19) with respect to a plurality of network elements (e.g. IP address, electronic storefront domain name, shipping address, contact information, browser software, credit card, transaction amount, time-of-day, day-of-week, etc.), identifying network elements associated with a requested on-line resource, and determining a score based on the authentication patterns with the identified network elements (e.g. block S808, page 37, lines 10-19).

As further set forth in dependent claims 46, 48 and 50, the process of determining a score includes applying a weight to network elements based on their relative importance, evaluating the user's historical relationship with the network elements, and determining the user's score based on the weighted evaluation (e.g. blocks S806, S808, page 35, line 7 to page 38, line 4).

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Independent claims 1, 20, 39 stand rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,931,402 Pereira III et al. ("Pereira") in view of U.S. Patent No. 5,784,566 Viavant et al. ("Viavant"). Claims 2, 7, 8, 21, 26, 27, 40, and 43 stand rejected under 35 U.S.C. 103(a) as being allegedly unpatentable over Pereira in view of Viavant and U.S. Patent 6,157,707 Baulier et al. ("Baulier"). Claims 10-16 and 29-35 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Pereira III in view of Viavant and U.S. Patent 5,708,422 Blonder et al. ("Blonder"). Claims 46-51 stand rejected under 35 U.S.C. 103(a) as being allegedly

unpatentable over Pereira III in view of Viavant and Baulier and U.S. Patent 6,466,918 to Spiegel et al.. ("Spiegel"). Appellants respectfully submit that these rejections are in error for multiple reasons, and seek review of the following independently reversible grounds:

- Whether Pereira or Viavant, alone or in combination, disclose or suggest all of the following claim limitations of independent claims 1, 20 and 39:
    - storing business rules for a plurality of companies having on-line resources,
    - identifying a company associated with a requested on-line resource from among the plurality of companies,
    - retrieving the stored business rules for the identified company, and
    - determining whether stored business rules for the identified company associated with the requested on-line resource indicates that authentication for the user is required.
- Whether Pereira, Viavant and Baulier, alone or in combination, disclose or suggest storing a profile of a user's authentication patterns, identifying network elements associated with a requested on-line resource, and determining a score based on the authentication patterns with the identified network elements, as required by claims 2, 21 and 40.
- Whether Pereira, Viavant, Baulier and Spiegel, alone or in combination, disclose or suggest applying a weight to network elements based on their relative importance, evaluating the user's historical relationship with the network elements, and determining the user's score based on the weighted evaluation, as required by claims 46, 48 and 50.

ARGUMENT

The present claims patentably define over the cited prior art because these references, alone or in combination, do not disclose or suggest each and every limitation of the claims. Meanwhile, a *prima facie* case of obviousness under § 103 requires that each and every limitation be taught or suggested in the cited prior art. MPEP 2143.03; *In re Royka*, 490 F.2d 981 (CCPA 1974). Accordingly, the § 103 rejections of the claims should be reversed.

Pereira and Viavant, Alone Or In Combination, Do Not Disclose Or Suggest Each and Every Limitation Of Independent Claims 1, 20 and 39

The § 103 rejections of the independent claims 1, 20 and 39 based on Pereira and Viavant should be reversed because each and every limitation is not found in the cited prior art, and so a *prima facie* case of obviousness under § 103 has not been made.

Independent Claims 1, 20 and 39 Require Storing Business Rules For A Plurality of Companies And Determining Whether A Request For An On-Line Resource Requires Authentication Based On The Stored Business Rules For The Company Identified As Being Associated With The Requested On-Line Resource

Independent claim 1 explicitly requires (with similar limitations in claims 20 and 39):

> A method for reducing the occurrence of unauthorized use of on-line resources, comprising:
>
> [1] storing business rules for a plurality of companies having on-line resources;
>
> receiving a message indicating a request from a user to use on-line resources;
>
> [2] identifying a company associated with the requested on-line resource from among the plurality of companies;
>
> [3] retrieving the stored business rules for the identified company
>
> ...
>
> wherein the step of determining whether the request requires authentication includes [4] determining whether stored business rules for the identified company associated with the requested on-line resource indicates that authentication for the user is required.

Accordingly, the independent claims clearly define a method and system that stores business rules for a plurality of companies having on-line resources, the business rules being retrieved by identifying the particular company associated with a user request for on-line resources, the retrieved rules of the identified company being used to determine whether authentication is required for a requested on-line resource.

Pereira Alone Does Not Teach Or Suggest All Claim Limitations

Pereira teaches a system for creating and storing profiles of users who may use a single company's extranet to access objects in a database of that company, in which those accessing users may belong to different companies other than that single company. Pereira teaches nothing about determining whether authentication is needed, as the Office Action correctly admits.

However, the Office Action wrongly alleges that Pereira teaches controlling access to on-line resources of one of a plurality of companies associated with a given user request.

Pereira teaches the storage and construction of user profile records for "controlling access for a plurality of users to a plurality of objects located in at least one electronic database." (col. 2 lines 18-22). As explained at col. 3, line 62 to col. 4, line 5, "The profiling system processor 18 receives the requests for access to an object that is controlled by the profiling system via the communication link 11. The profiling system then determines whether to grant the user access to an object by retrieving one or more profile system database records that correspond to the user and object to be accessed where the profile system database records are similar to those shown in FIGS. 1-3 (and described below). Once the profiling system determines (or resolves) that the user is entitled to the requested form of access for the object, the user is granted such access."

Nothing in Pereira teaches or suggests controlling access to on-line resources of different companies, much less in accordance with the limitations of the independent claims. Specifically, Pereira does not teach or suggest [1] storing business rules for a plurality of companies, [2] identifying a company associated with the requested on-line resource from among the plurality of companies; [3] retrieving stored business rules for the identified company; or [4] determining whether stored business rules for the identified company associated with the requested on-line resource indicates that authentication for the user is required.

Taking limitations [1] and [4] together, for example, the independent claims clearly require that rules for determining whether authentication is required for a requested access must be stored for a plurality of companies having on-line resources. With respect to these limitations, the Office Action implicitly admits they are missing from Pereira by rewriting the claim language to say that "Pereira III teaches storing business rules for a plurality of users of different companies." (Action at 2, emphasis added) Meanwhile, the claim requires storing rules for a plurality of companies, not rules for a plurality of users as stated in the Office Action. Moreover, by clear logic and claim antecedence, the stored rules must be useful for determining whether authentication is performed. Accordingly, Pereira does not teach or suggest [1] storing business rules for a plurality of companies.

Even if, *arguendo*, certain objects in database 14 controlled by Pereira's profiling system could be considered as belonging to different companies, there is no teaching or suggestion in

Pereira of identifying a company associated with a requested on-line resource (i.e. database 14), and retrieving rules for the identified company associated with the requested on-line resource as further required by limitations [2] and [3]. The Office Action again resorts to rewriting the claim language by stating that "Pereira III teaches retrieving the rules according to the user." (Action at 3, emphasis added). Meanwhile the claim requires retrieving rules for the identified company, wherein the company is identified from the requested on-line resource.

The Office Action may have misinterpreted Pereira's descriptions at col. 5, lines 27-37, and FIG. 3 which teaches:

> In the Matrix database the attributes may control access to a specific object or group of objects. Note, for example the fourth record in the database for user3, identified as associated with Company C in the vertical component database. The user has a "Company" attribute in the Matrix database equal to "Company A", an "Access" attribute equal to "Read-Only", and a "Role" attribute equal to "Role1". Thus, user3 has conditional Read-Only access to Company A objects for the Role "Role1" where as explained below with reference to FIG. 3, users having the value "Role1" for the Role attribute may access the objects for Function1 and Function2.

At best, this merely indicates that some objects in the database 14 may be grouped according to different companies, and that access to such groups of objects can be separately controlled. However, these database objects are all within the single company's (e.g. Company A) on-line database 14. This does not teach or suggest storing or retrieving rules for accessing databases (the alleged "on-line resource") of a plurality of different companies (e.g. Company B's or C's databases). This merely describes profiles for accessing different objects in one database (the alleged "on-line resource") of a single company (e.g. Company A).

As properly understood, Pereira does not even need, and so does not suggest, identifying a company associated with a requested on-line resource, or retrieving rules for that identified company. When a user requests access to objects in database 14, Pereira merely obtains a profile for how objects in that database 14 (the alleged "on-line resource") can be accessed by that user. There is no need to identify an "on-line resource" (e.g. database 14) at all, much less identifying database 14 of Company A from among databases belonging to different companies (e.g. Company B or C). Moreover, the requested object itself determines the group to which it

belongs, and the user's profile determines the access to the object. Accordingly, at best, Pereira suggests retrieving access rules for the user and object, and there is no need or suggestion for retrieving rules for an identified company.

In sum, the Office Action admits that Pereira does not teach or suggest determining whether authentication is required for a given requested access from stored business rules for a company associated with that request. By antecedent basis and clear logical extension, this further means that Pereira does not teach or suggest storing such rules from which such a determination can be made, and so Pereira does not teach or suggest at least limitations [1] and [4] of the independent claims.

Moreover, as shown above, the Office Action's allegations that Pereira teaches [2] identifying a company associated with the requested on-line resource from among the plurality of companies; and [3] retrieving stored business rules for the identified company are in error. Accordingly, Pereira does not fairly teach or suggest any of these limitations of independent claims 1, 20 and 39.

Viavant Alone Does Not Teach Or Suggest All Claim Limitations

Viavant is cited for allegedly teaching "determining whether a request requires authentication." However, the claim requires much more. It requires that the step of determining whether the request requires authentication includes [4] determining whether stored business rules for the identified company associated with the requested on-line resource indicates that authentication for the user is required.

The Office Action admits that Pereira does not teach anything about authentication. However, the Office Action wrongly alleges that Viavant cures the deficiencies of Pereira in meeting this subject matter.

Viavant merely teaches a system and method for providing security services between a client and server in a network. There is no teaching or suggestion of [1] storing business rules for a plurality of companies, [2] identifying a company associated with a requested on-line resource from among the plurality of companies, or [3] retrieving stored business rules for the identified company, as correctly admitted by the Office Action.

Viavant teaches that a client and server negotiate an authentication service to use for a particular communication session. The client and server each share their "preferences" for a particular authentication method. The preferences can include whether a particular form of authentication is required or not. Depending on their exchange of preferences, a form of authentication is chosen, or either none is required or they cannot agree on a form and one is required, in which case the communication fails. (see col. 6, lines 43-66).

At best, Viavant teaches determining whether authentication is required for a session between one client and one server. Nothing in Viavant, however, suggests that such determination includes [4] determining whether stored business rules for the identified company associated with the requested on-line resource indicates that authentication for the user is required. Accordingly, Viavant's teachings fall short of meeting the limitations of the claims.

The Alleged Combination Of Pereira and Viavant Would Not Suggest the Claimed Invention

As set forth above, the Office Action admits that Pereira does not teach anything about authentication, and Viavant does not suggest [4] determining whether stored business rules for the identified company associated with the requested on-line resource indicates that authentication for the user is required. Accordingly, all limitations of the claims are not met by the alleged combination of Pereira and Viavant for at least this reason. Nevertheless, for additional reasons set forth above, it is respectfully submitted that Pereira and Viavant do not disclose or suggest limitations [1], [2], or [3] either. Accordingly, the Office Action has not established a *prima facie* case of obviousness against the independent claims and all pending rejections should be reversed for at least this reason.

Pereira, Viavant and Baulier Do Not Disclose Or Suggest Storing A Profile Of A User's Authentication Patterns, Identifying Network Elements Associated With A Requested On-Line Resource, And Determining A Score Based On The Authentication Patterns With The Identified Network Elements, As Required By Claims 2, 21 And 40

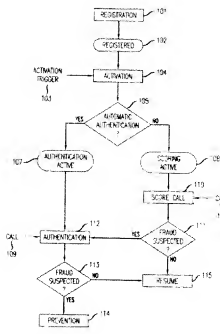
Dependent claims 2, 21 and 40 depend from independent claims 1, 20 and 39, and so are patentable for at least the reasons presented above.

Dependent claims 2, 21 and 40 further require, *inter alia*, [5] storing a profile of a user's authentication patterns with respect to a plurality of network elements, [6] identifying a network element from among network elements in the stored profile associated with a requested on-line resource, and [7] determining a score based on the authentication patterns with the identified network elements.

The Office Action admits that these limitations are not found in Pereira or Viavant, and relies on Baulier in support of its rejections.

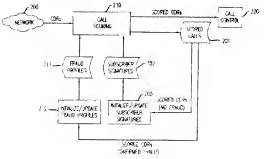
Baulier merely compares a telephone caller's calling patterns with a fraud profile to determine whether a particular telephone call is fraudulent. FIG. 1, reproduced here, shows how Baulier allows "selective authentication" to be performed versus "automatic authentication" for a given subscriber. If selective authentication is to be performed (NO in step 105), call scoring can be performed on a subscriber's call. If fraud is suspected in accordance with the score, then authentication can be performed.

FIG. 1



Moreover, nothing in Baulier teaches anything about storing authentication patterns for a user, much less with respect to a plurality of network elements, and much less determining a score based on these patterns. FIG. 2 showing Baulier's call scoring is reproduced here.

FIG. 2



As shown and described in connection with FIG. 2, Baulier merely teaches forming an updated "subscriber signature" which is based on call detail records (CDRs), and comparing that signature against a fraud profile. As further set forth in col. 6, line 59 to col. 7, line 8, Baulier teaches nothing about including authentication patterns in the "subscriber signature":

> It should also be noted that a subscriber signature may monitor many aspects of a subscriber's calling behavior including, but not limited to: calling rate, day of week timing, hour of day timing, call duration, method of billing, geography, and so on. Consequently, a signature may be derived from information that is typically contained within the call detail records, such as: originating number; terminating number; billed number; start time and date; originating location; carrier selection; call waiting indicators; call forwarding indicators; three-way calling/transfer indicators; operator assistance requests; and network security failure indicators, to name a few. The particular elements to be used for establishing and updating a subscriber signature may depend on the type of network (e.g., wireline, wireless, calling card, non-telecommunication, etc.), the particular scoring method being used, as well as other factors that would be apparent to those skilled in the art.

Baulier also discusses authentication techniques that may be used for a given call. So Baulier clearly distinguishes between information about calls, and authentication applied to calls. Baulier does not suggest anything about storing results of authentication, it merely stores processed call information. Moreover, although Baulier teaches that how a subscriber signature is updated may depend on a type of network being used for the call, Baulier teaches and suggests nothing about storing separate subscriber signatures for such different networks even if, *arguendo*, the signature could be viewed as the claimed authentication patterns. Accordingly, Baulier does not suggest [5] storing a profile of a user's authentication patterns with respect to a plurality of network elements.

Finally, as clearly shown above, Baulier's "score" is determined based on a comparison of a "subscriber signature" with a "fraud profile". Baulier teaches nothing about accounting for past authentication results in the process of determining a score, and so cannot teach or suggest [7] "determining a score for the user based on the user's historical authentication patterns with the certain network elements" as required by claims 2, 21 and 40.

Accordingly, it is respectfully submitted that Pereira, Viavant and Baulier do not disclose or suggest at least limitations [5] or [7] as set forth above. Accordingly, the Office Action has not established a *prima facie* case of obviousness against claims 2, 21 and 40, and the rejections

thereof, as well as the rejections of claims 46-51 that depend therefrom, should be reversed for at least this additional independent ground.

Pereira, Viavant, Baulier and Siegel Do Not Disclose Or Suggest Applying A Weight To Network Elements Based On Their Relative Importance, Evaluating The User's Historical Relationship With The Network Elements, And Determining The User's Score Based On The Weighted Evaluation, As Required By Claims 46, 48 and 50

Dependent claims 46, 48 and 50 depend from claims 2, 21, and 40, respectively, which further depend from independent claims 1, 20 and 39, and so are patentable for at least the reasons presented above.

Dependent claims 46, 48 and 50 further require, *inter alia*, [8] applying a weight to network elements based on their relative importance, [9] evaluating the user's historical relationship with the network elements, and [10] determining the user's score based on the weighted evaluation.

The Office Action strings together a tenuous collection of four references to support its rejections of these claims. However, it relies on only Singer as suggesting the above subject matter. This reliance is misplaced.

Spiegel (assignee is Amazon.com) merely tracks a user's historical activities with respect to a website. Weights are applied to certain activities (e.g. purchase, click-through, etc.) based on their relative importance. Weighted scores of the activities are tracked for different book categories (apparently the alleged "network elements"). For convenience, Table 6 of Spiegel is reproduced below.

TABLE 6

Book Category	Purchase (210)	Click-Through (211)	Search (203)	Rating (208)	Shopping Cart (207)	Weighted Scores
Air Sports & Recreation	(0 * 210) +	(0 * 211) +	(3 * 203) +	(0 * 208) +	(0 * 207) =	0
Audiobooks	(3 * 210) +	(24 * 211) +	(35 * 203) +	(3 * 208) +	(7 * 207) =	14632
Automotive	(0 * 210) +	(19 * 211) +	(21 * 203) +	(0 * 208) +	(0 * 207) =	8082
Reference	(0 * 210) +	(0 * 211) +	(3 * 203) +	(0 * 208) +	(0 * 207) =	0
Scuba	(0 * 210) +	(0 * 211) +	(3 * 203) +	(0 * 208) +	(0 * 207) =	0
Swimming	(8 * 210) +	(73 * 211) +	(57 * 203) +	(12 * 208) +	(6 * 207) =	31662
Yoga	(0 * 210) +	(0 * 211) +	(3 * 203) +	(0 * 208) +	(0 * 207) =	0

Accordingly, even if, *arguendo*, Spiegel's "book category" could correspond to the claimed network element, Spiegel would not disclose or suggest at least [8] applying a weight to network elements based on their relative importance, and [10] determining the user's score based on the weighted evaluation, as required by claims 46, 48 and 50.

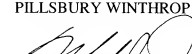
It is therefore respectfully submitted that Pereira, Viavant, Baulier and Spiegel do not disclose or suggest at least limitations [8] or [10] as set forth above. Accordingly, the Office Action has not established a *prima facie* case of obviousness against claims 46, 48 and 50, and the rejections thereof should be reversed for at least this additional independent ground.

CONCLUSION

For the foregoing reasons, Appellants respectfully request that all the pending claims be deemed allowable by this honorable Board.

Respectfully submitted,
PILLSBURY WINTHROP SHAW PITTMAN LLP

Date: May 30, 2006



40,580
Reg. No.

Mark J. Danielson
Telephone: (650) 233-4777
Facsimile: (650) 233-4545
Please reply to customer no. 27,498

CLAIMS APPENDIX

1. (Previously presented) A method for reducing the occurrence of unauthorized use of on-line resources, comprising:

storing business rules for a plurality of companies having on-line resources;

receiving a message indicating a request from a user to use on-line resources;

identifying a company associated with the requested on-line resource from among the plurality of companies;

retrieving the stored business rules for the identified company;

determining whether the request requires authentication;

enabling the request to be fulfilled without authentication if the determination indicates that authentication is not required;

obtaining an indicia of physical identification from the user if the determination instead indicates that authentication is required;

comparing the obtained indicia to a stored indicia for the user; and

enabling the request to be fulfilled if the obtained indicia matches the stored indicia,

wherein the step of determining whether the request requires authentication includes determining whether stored business rules for the identified company associated with the requested on-line resource indicates that authentication for the user is required.

2. (Previously presented) A method according to claim 1, wherein the step of determining whether the request requires authentication includes:

retrieving a stored profile containing the user's historical authentication patterns with respect to a plurality of network elements;

identifying certain network elements of the plurality of network elements in the stored profile as being associated with the requested on-line resource;

determining a score for the user based on the user's historical authentication patterns with the certain network elements; and

determining whether authentication is required for this request to use the on-line resource based on the score.

3. (Canceled)

4. (Previously presented) A method according to claim 1, wherein the step of determining whether the stored business rules requires authentication includes:

determining whether the user is listed by the company as always requiring authentication; and

requiring authentication if the user is listed.

5. (Previously presented) A method according to claim 1, wherein the step of determining whether the stored business rules requires authentication includes:

determining whether the user is listed by the company as never requiring authentication; and

not requiring authentication if the user is listed.

6. (Previously presented) A method according to claim 1, wherein the step of determining whether the stored business rules requires authentication includes:

determining whether the user is listed by the company as being completely denied access; and

completely denying access to the requested on-line resources if the user is listed.

7. (Original) A method according to claim 1, wherein the step of determining whether the request requires authentication includes determining whether the request is indicative of fraudulent behavior.

8. (Original) A method according to claim 7, wherein the fraudulent behavior is one or more of a collision violation, a velocity violation, and a customized trigger.

9. (Canceled)

10. (Previously presented) A method according to claim 1, further comprising:

determining whether the request is a card transaction;

determining whether restrictions applied to the user and an account associated with the request are satisfied by a purchase associated with the request; and

denying the request if the restrictions are not satisfied.

11. (Original) A method according to claim 10, wherein the restrictions are one or more of type of goods to be purchased, amount of purchase, time of purchase and location of purchase.

12. (Previously presented) A method according to claim 1, further comprising:

determining whether the request is an account transaction;

determining whether restrictions applied to an account associated with the account transaction are satisfied by the request; and

denying the request if the restrictions are not satisfied.

13. (Original) A method according to claim 12, wherein the restrictions are one or more of frequency of access and time of access.

14. (Previously presented) A method according to claim 1, further comprising:

determining whether the request is an account transaction;

determining whether use of the requested on-line resources are restricted for an account associated with the user; and

denying the request if the requested on-line resources are restricted for the account.

15. (Previously presented) A method according to claim 1, further comprising:

determining whether the request is a control transaction;

determining whether restrictions applied to the user associated with the control transaction are satisfied by the request; and

denying the request if the restrictions are not satisfied.

16. (Original) A method according to claim 15, wherein the restrictions are one or more of a parent control and an other control.

17. (Canceled)

18. (Previously presented) A method according to claim 1, wherein the indicia comprises a biometric that is one or more of a fingerprint, a voiceprint, a palmprint, an eye scan, and a handwriting sample.

19. (Previously presented) A method according to claim 1, further comprising providing access to the plurality of companies to allow them to configure their own individual set of stored business rules that are used in the determining step.

20. (Previously presented) An apparatus for reducing the occurrence of unauthorized use of on-line resources, comprising:

means for storing business rules for a plurality of companies having on-line resources;

means for receiving a message indicating a request from a user to use on-line resources;

means for identifying a company associated with the requested on-line resource from among the plurality of companies;

means for retrieving the stored business rules for the identified company;

means for determining whether the request requires authentication;

means for enabling the request to be fulfilled without authentication if the determination indicates that authentication is not required;

means for obtaining an indicia of physical identification from the user if the determination instead indicates that authentication is required;

means for comparing the obtained indicia to a stored indicia for the user; and

means for enabling the request if the obtained indicia matches the stored indicia,

wherein the means for determining whether the request requires authentication includes means for determining whether stored business rules for the identified company associated with the requested on-line resource indicates that authentication for the user is required.

21. (Previously presented) An apparatus according to claim 20, wherein the means for determining whether the request requires authentication includes:

means for retrieving a stored profile containing the user's historical authentication patterns with respect to a plurality of network elements;

means for identifying certain network elements of the plurality of network elements in the stored profile as being associated with the requested on-line resource;

means for determining a score for the user based on the user's historical authentication patterns with the certain network elements; and

means for determining whether authentication is required for this request to use the on-line resource based on the score.

22. (Canceled)

23. (Previously presented) An apparatus according to claim 20, wherein the means for determining whether the stored business rules requires authentication includes:

means for determining whether the user is listed by the company as always requiring authentication; and

means for requiring authentication if the user is listed.

24. (Previously presented) An apparatus according to claim 20, wherein the means for determining whether the stored business rules requires authentication includes:

means for determining whether the user is listed by the company as never requiring authentication; and

means for not requiring authentication if the user is listed.

25. (Previously presented) An apparatus according to claim 20, wherein the means for determining whether the stored business rules requires authentication includes:

means for determining whether the user is listed by the company as being completely denied access; and

means for completely denying access to the requested on-line resources if the user is listed.

26. (Original) An apparatus according to claim 20, wherein the means for determining whether the request requires authentication includes means for determining whether the request is indicative of fraudulent behavior.

27. (Original) An apparatus according to claim 26, wherein the fraudulent behavior is one or more of a collision violation, a velocity violation, and a customized trigger.

28. (Canceled)

29. (Previously presented) An apparatus according to claim 20, further comprising:

means for determining whether the request is a card transaction;

means for determining whether restrictions applied to the user and an account associated with the request are satisfied by a purchase associated with the request; and

means for denying the request if the restrictions are not satisfied.

30. (Original) An apparatus according to claim 29, wherein the restrictions are one or more of type of goods to be purchased, amount of purchase, time of purchase and location of purchase.

31. (Previously presented) An apparatus according to claim 20, further comprising:

means for determining whether the request is an account transaction;

means for determining whether restrictions applied to an account associated with the account transaction are satisfied by the request; and

means for denying the request if the restrictions are not satisfied.

32. (Original) An apparatus according to claim 31, wherein the restrictions are one or more of frequency of access and time of access.

33. (Previously presented) An apparatus according to claim 20, further comprising:

means for determining whether the request is an account transaction;

means for determining whether use of the requested on-line resources are restricted for an account associated with the user; and

means for denying the request if the requested on-line resources are restricted for the account.

34. (Previously presented) An apparatus according to claim 20, further comprising:

means for determining whether the request is a control transaction;

means for determining whether restrictions applied to the user associated with the control transaction are satisfied by the request; and

means for denying the request if the restrictions are not satisfied.

35. (Original) An apparatus according to claim 34, wherein the restrictions are one or more of a parent control and an other control.

36. (Canceled)

37. (Previously presented) An apparatus according to claim 35, wherein the indicia comprises a biometric that is one or more of a fingerprint, a voiceprint, a palmprint, an eye scan, and a handwriting sample.

38. (Previously presented) An apparatus according to claim 20, further comprising means for providing access to the plurality of companies to allow them to configure their own individual set of stored business rules that are used by the determining.

39. (Previously presented) An apparatus for reducing the occurrence of unauthorized use of on-line resources, comprising:

a server that is adapted to communicate with a network based service so as to receive a message indicating a request from a user to use the network based service;

a rules subsystem coupled to the server that determines whether the request requires authentication, the rules subsystem causing the server to enable the request to be fulfilled without authentication if the determination indicates that authentication is not required and causes the server to obtain an indicia of physical identification from the user if the rules subsystem instead determines that authentication is required; and

a business rules database coupled to the rules subsystem, the database storing business rules for a plurality of companies having on-line resources;

an authentication subsystem coupled to the server that compares the obtained indicia to a stored indicia for the user,

wherein the rules subsystem is adapted to identify a company associated with the requested on-line resource from among the plurality of companies, retrieve the stored business rules for the identified company from the business rules database and determine whether the stored business rules for the identified company associated with the requested on-line resource requires authentication for the user, and

wherein the server sends a signal to the network based service that the request is to be fulfilled if the authentication subsystem determines that the obtained indicia matches the stored indicia.

40. (Previously presented) An apparatus according to claim 39, further comprising:

a profile database coupled to the rules subsystem, the profile database maintaining a stored profile containing the user's historical authentication patterns with respect to a plurality of network elements,

wherein the rules subsystem is adapted to retrieve the user's stored profile from the profile database in response to the request, identify certain network elements of the plurality of network elements in the stored profile as being associated with the requested on-line resource, determine a score for the user based on the user's historical authentication patterns with the certain network elements, and to determine whether authentication is required for the user for this request to use the on-line resource based on the score.

41-42. (Canceled)

43. (Previously Presented) An apparatus according to claim 39, further comprising a user profile subsystem coupled to the server which is adapted to determine whether the request is indicative of fraudulent behavior, wherein the fraudulent behavior is one or more of a collision violation, a velocity violation, and a customized trigger.

44. (Canceled)

45. (Previously presented) An apparatus according to claim 39, wherein the indicia is a biometric, the apparatus further comprising a biometrics database that stores a plurality of biometrics for a respective plurality of users, and wherein the plurality of biometrics includes one or more of a fingerprint, a voiceprint, a palmprint, an eye scan, and a handwriting sample.

46. (Previously Presented) A method according to claim 2, wherein the step of determining the score includes:

applying a weight to each of the certain network elements based on a relative importance of the certain network elements;

evaluating the user's historical relationship with each of the certain network elements; and

aggregating the score using the weighted evaluations.

47. (Previously Presented) A method according to claim 46, further comprising:

allowing a system administrator to configure the respective weights for the plurality of network elements.

48. (Previously Presented) An apparatus according to claim 21, wherein the means for determining the score includes:

means applying a weight to each of the certain network elements based on a relative importance of the certain network elements;

means evaluating the user's historical relationship with each of the certain network elements; and

means for aggregating the score using the weighted evaluations.

49. (Previously Presented) An apparatus according to claim 48, further comprising:

means for allowing a system administrator to configure the respective weights for the plurality of network elements.

50. (Previously presented) An apparatus according to claim 39, wherein the rules subsystem is further adapted to apply a weight to each of the certain network elements based on a relative importance of the certain network elements, evaluate the user's historical relationship with each of the certain network elements, and aggregate the score using the weighted evaluations.

51. (Previously Presented) An apparatus according to claim 50, further comprising:

an administrator service that allows a system administrator to configure the respective weights for the plurality of network elements.

EVIDENCE APPENDIX

RELATED PROCEEDINGS APPENDIX